

## UNITED STATES DISTRICT COURT

for the

Northern District of Oklahoma

In the Matter of the Search of  
 a black Chevrolet Silverado Trail Boss,  
 VIN: 1GCPYCEF1MZ308995

)  
)  
)  
)  
)

Case No.

24-mj-75-SH

**FILED UNDER SEAL**

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

See Attachment "A2"

located in the Northern District of Oklahoma, there is now concealed (*identify the person or describe the property to be seized*):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

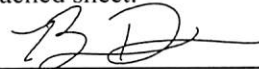
18 U.S.C. §§ 2252(a)(4)(B), and  
 (b)(2)

Possession of and Access with Intent to View Child Pornography

The application is based on these facts:

See Affidavit of FBI SA Brian S. Dean, attached hereto.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 \_\_\_\_ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

Special Agent Brian S. Dean, FBI

Printed name and title

Subscribed and sworn to by phone.

Date:

2/1/24



Judge's signature

City and state: Tulsa, Oklahoma

Susan E. Hunstman, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

**In the Matter of the Search of the  
Person of Bobby Neal Temple Jr., a  
black Chevrolet Silverado Trail Boss,  
VIN: 1GCPYCEF1MZ308995, and the  
complete premises located at 402 S.  
14th St., Collinsville, Oklahoma 74021**

Case No. \_\_\_\_\_

**FILED UNDER SEAL**

**Affidavit in Support of an Application  
Under Rule 41 for a Warrant to Search and Seize**

I, Brian S. Dean, being first duly sworn under oath, depose and state:

**Introduction and Agent Background**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for three separate search warrants for (1) the person of Bobby Neal Temple Jr. (“**TEMPLE**”), (2) a black Chevrolet Silverado truck, Trail Boss edition, with VIN: 1GCPYCEF1MZ308995 and a paper tag (“**TARGET VEHICLE**”), and (3) the entire property located at **402 S. 14<sup>th</sup> St., Collinsville, OK 74021**, to include outbuildings and vehicles on the curtilage premises (“**TARGET RESIDENCE**”); as described in separate Attachments A1, A2, and A3 for the items further detailed in Attachment B.

2. I am a federal law enforcement officer as defined under Rule 41(a)(2)(C) and am authorized to request these search warrants because I am a government agent who is engaged in enforcing federal criminal laws and I am within the category of

officers authorized by the Attorney General to request such warrants. I am a Special Agent with the Federal Bureau of Investigation assigned to the Oklahoma Safe Streets Task Force based in Tulsa, Oklahoma. As a Special Agent, my duties include investigating violations of federal criminal law and threats to national security. In addition to formalized training, I have received extensive training through my involvement in an array of investigations working alongside experienced law enforcement officers at both the federal and local level. My investigations include, but are not limited to, drug and gang violations, violent crimes, Indian country violations, counterterrorism, cybercrimes, and crimes against children.

3. Specifically, I have extensive experience working cases involving child pornography and child exploitation in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. All of these cases have required the review of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. As such, I am familiar with the tactics utilized by individuals who collect, distribute, and/or produce child pornographic material.

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application

for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. Based on my training, experience, and the facts set forth in this affidavit, there is probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) will be located in medium maintained either on **TEMPLE's** person and/or in the associated **TARGET VEHICLE** or **TARGET RESIDENCE**, as further described in Attachments A1, A2, and A3.

#### **Jurisdiction**

6. “[A] warrant may be issued to search for and seize any property that constitutes evidence of a criminal offense in violation of the laws of the United States.” 18 U.S.C. § 3103a.

7. The requested search is related to the following violations of federal law:

a. Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) prohibit any person from knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, one or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if the production of such visual depiction involved the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct.

8. Venue is proper because the person and/or property described in this affidavit is located within the Northern District of Oklahoma. Fed. R. Crim. P. 41(b)(1).

### **Definitions**

9. The following definitions, inclusive of all definitions contained in 18 U.S.C. § 2256, apply to this affidavit and the attachments incorporated herein:

a. “Child pornography,” as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct;

b. “Cloud storage service” refers to a publicly accessible, online storage provider that can be used to store and share files in large volumes. Users of cloud storage services can share links and associated passwords to their stored files with others in order to grant access to their file collections. Such services allow individuals to easily access these files through a wide variety of electronic devices such as desktop computers, laptops, mobile phones or tablets, from anywhere. Many services provide free access up to a certain size limit;

- c. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state;
- d. “Minor,” as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years;
- e. “Records,” “documents,” and “materials,” as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form;
- f. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person; and
- g. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

h. “Computer,” as defined in 18 U.S.C. § 1030(e)(1), means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

### **Probable Cause**

10. In late November 2023, FBI Tulsa was contacted by an individual, hereinafter WITNESS 1, who claimed her father, **Bobby Neal Temple Jr.**, (DOB: XX/XX/1961; SSN: XXX/XX/5616) was in in possession of material which would constitute as child pornography.<sup>1</sup> WITNESS 1 said in December 2022, while visiting **TEMPLE** in the hospital, she accessed his phone, described as a black in color Android or non-Apple device, while he was asleep looking for photos of her brother who had just recently passed away. While scrolling through the photo library, WITNESS 1 came across an image of her sister, **TEMPLE’s** step-daughter, hereinafter VICTIM 1, fully nude and posing in a sexually suggestive manner. WITNESS 1 said the image appeared to have been taken in a bedroom from her childhood home, and estimated VICTIM 1 was between 12-14 years old in the

---

<sup>1</sup> 18 U.S.C. § 2252 prohibits certain acts, such as possession and distribution, of visual depictions of a minor, that is, a person under the age of 18, engaged in sexually explicit conduct. 18 U.S.C. § 2256(2)(A) defines explicit conduct,” and includes sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area.

photo. Victim 1 was born in 1998, which would make the photo approximately 10-12 years old at the time of discovery.

11. WITNESS 1 “froze” when she found the image, and immediately stopped scrolling through the photos. She put the phone down and never re-accessed the device, and so she was therefore unsure if there were any additional images and/or victims depicted on the device. WITNESS 1 explained **TEMPLE** was scheduled to come live with her at the **TARGET RESIDENCE** after he got out of the hospital, and so she was afraid to confront him with what she saw. She said she hoped she could just move on and forget about it, as she no longer shared a relationship with VICTIM 1, but for the next several months, WITNESS 1 struggled silently. WITNESS 1 also recalled that several years after her mother and **TEMPLE** separated, VICTIM 1 came forward and alleged **TEMPLE** had sexually molested her. WITNESS 1 was unaware of what VICTIM 1 specifically told law enforcement, but she could not shake the thought that the photo she observed on **TEMPLE**’s phone gave credence to VICTIM 1’s claims.

12. FBI Tulsa subsequently conducted a cursory review of state and local law enforcement reporting and identified multiple relevant reports. In 2014, (Oklahoma City Police Incident Report 2014-0027690) VICTIM 1 accused **TEMPLE** of repeat molestation beginning when she was approximately 8 years old and continuing until she was approximately 13 years old. Despite VICTIM 1’s claims, there was not enough additional evidence to pursue charges against **TEMPLE**. FBI Tulsa also

located a report from several years prior in 2012 (OCPD Incident Report 2012-0022599) where VICTIM 1 was engaged in graphic sexual communications with a 19 y/o male via social media. In the report, it is clear VICTIM 1 at the age of 14, was hyper-sexualized, engaging in both physical contact and graphic communications with several older boys and young men. Based on training and experience, your affiant knows sexualized behavior displayed at a young age can be indicative of prior exposure and possible abuse. Children who have abused will often sub-consciously associate their sense of self-worth with the attention garnered from such behavior.

13. After more than six months attempting to help **TEMPLE** get back on his feet and off his drug habit, WITNESS 1 finally had enough and moved out of the **TARGET RESIDENCE**, cutting off all further contact with **TEMPLE**. WITNESS 1 described **TEMPLE** as manipulative, verbally abusive, and claimed he had pointed a loaded firearm at her during an argument, although she never reported the matter to law enforcement. She said she was intimidated by **TEMPLE**, and it was not until she was fully removed from his influence did she feel confident enough to talk about, and eventually report, what she saw on **TEMPLE**'s phone. WITNESS 1 said **TEMPLE** was still in possession of this device when she moved out, but she had not had any contact with him since and knew **TEMPLE** occasionally moved SIM cards from handset to handset.

14. In January 2024, WITNESS 1 said **TEMPLE** had been served an official notice of eviction and was no longer permitted to live in the **TARGET RESIDENCE**. WITNESS 1 confirmed while she had changed the locks, the majority of **TEMPLE**'s personal effects were still located inside the **TARGET RESIDENCE**, and he was now allegedly sleeping in his vehicle, described as a black Chevrolet Silverado truck, Trail Boss edition, with a paper tag (**TARGET VEHICLE**), across the street in a trailer park. On January 22, 2024, FBI Tulsa conducted physical surveillance and identified the **TARGET VEHICLE** parked across the street from the **TARGET RESIDENCE**, and on January 25, 2024, local law enforcement confirmed **TEMPLE** was indeed sleeping in the **TARGET VEHICLE** after returning a dog to him at that location.

**Characteristics Common to Individuals  
who Exhibit a Sexual Interest in Children and Individuals who Distribute,  
Receive, Possess and/or Access with Intent to View Child Pornography**

15. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view child pornography:

- a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in

person, in photographs, or other visual media, or from literature describing such activity;

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts;

c. Such individuals almost always possess and maintain digital or electronic files of child pornographic material, that is, their pictures, videos, photographs, correspondence, mailing lists, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, videos, photographs, correspondence, and mailing lists for many years;

d. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer, phone, and/or surrounding area. These child pornography images are often maintained for years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person to enable the individual to have quick access to the child pornography images, which are

valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis;

e. Based on my training and experience and speaking with other special agents, I know that such individuals have taken their electronic devices and storage media, which contain their collections of child pornography, with them when they have moved or changed residences;

f. Such individuals may also take it upon themselves to create their own child pornography or child erotica images, videos, or other recordings, or engage in contact sex offenses with children. These images, videos or other recordings may be taken or recorded covertly, such as with a hidden camera in a bathroom, or the individual may have child victims he or she is abusing in order to produce child pornographic or child erotica images, videos or other recordings. Studies have shown there is a high cooccurrence between those who traffic in child pornography and commit sex offenses with children. Such individuals may also attempt to persuade, induce, entice, or coerce child victims in person or via communication devices to self-produce and send them child pornography or to meet in person for sex acts. These images, videos or other recordings are often collected, traded, or shared;

g. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through

the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted”<sup>2</sup> it;

h. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography;

i. Based on my training and experience, I know that such individuals may use their financial information to buy and sell child pornography online and purchase software used to mask their online activity from law enforcement. For instance, individuals may purchase cryptocurrency such as Bitcoin to buy and sell child pornography online. The use of cryptocurrency provides a level of anonymity because it masks the user’s identity when conducting online financial transactions and provides a means of laundering illicit proceeds. Financial information may provide a window into the identities of individuals seeking to buy or sell child pornography online by tying the illicit transactions back to the user. Financial

---

<sup>2</sup> See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because “staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology”); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

information contained on an electronic device containing child pornography may also provide indicia of ownership. Further, based on my training and experience, I know that individuals involved in the trafficking of child pornography may use sophisticated software, such as router configuration software, virtual private networks, proxy servers, cryptocurrency exchanges, or other anonymizing software, in conjunction with these illicit financial transactions to provide dual layers of anonymity and prevent law enforcement detection. Financial information may indicate which services were purchased to obscure an individual's identity;

j. Such individuals prefer not to be without their child pornography for any prolonged period of time. This behavior has been documented by law enforcement officers involved in similar investigations all throughout the world. Thus, even if **TEMPLE** has since acquired a new cell phone, the likelihood he no longer has access the image as described by WITNESS 1 after maintaining it for over a decade is slim. This prolonged maintenance is also indicative **TEMPLE** may have utilized cloud-based storage to ensure continued access no matter the status of his handset. It is therefore believed evidence of this access will be found either on his person, in the **TARGET VEHICLE**, or the **TARGET RESIDENCE**, as set forth in Attachments A1, A2, and A3.

**Background on Child Pornography, Computers,  
and the Internet**

16. Based on training, experience, and knowledge I have gleaned from other experienced law enforcement officers as it pertains to computer-related crimes, I know the following:

a. Computers, smartphones<sup>3</sup> and digital technology are the primary way in which individuals interested in child pornography interact with each other.

Computers and smartphones basically serve four functions in connection with child pornography: production, communication, distribution, and storage;

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as “WiFi” or “Bluetooth.” Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos;

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other

---

<sup>3</sup> Smartphones are a class of mobile phones and of multi-purpose mobile computing devices. They are distinguished from feature phones by their stronger hardware capabilities and extensive mobile operating systems, which facilitate wider software, internet (including web browsing over mobile broadband), and multimedia functionality (including music, video, cameras, and gaming), alongside core phone functions such as voice calls and text messaging.

computers via wireless connections. Electronic contact can be made to literally millions of computers and smartphones and tablets around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone;

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also almost always carried on an individual's person (or within their immediate dominion and control) and can additionally store media;

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion;

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as “cloud” storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user’s computer, smartphone or external media in most cases; and

g. As is the case with most digital technology, communications by way of computer or smartphone can be saved or stored on the computer or smartphone used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or smartphone, or saving the location of one’s favorite websites in, for example, “bookmarked” files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer or smartphone user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

### **Specifics of Search and Seizure of Computer Systems**

17. As described above and in Attachment B, this application seeks permission to search for records that might be found either on **TEMPLE's** person, in the associated **TARGET VEHICLE**, and/or in the **TARGET RESIDENCE** in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media, such as a cellular phone, smartphone, or tablet. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

18. I submit if a computer or storage medium is found on **TEMPLE's** person, in the **TARGET VEHICLE**, or the **TARGET RESIDENCE**, there is probable cause to believe records or images relevant to the ongoing investigation will be stored on said computer or storage medium, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data;

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file;

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information;

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

19. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrants, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any

storage medium found on **TEMPLE's** person, in the **TARGET VEHICLE**, and/or the **TARGET RESIDENCE** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified;

- b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information,

communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that logs the following: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection

logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement);

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when;

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer

behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant;

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent;

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

20. Based upon my training and experience and information provided to me by agents and others involved in the forensic examination of computers, I know computer data can be stored on a variety of computer systems and storage devices,

including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, smartphones, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to “cloud” storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;
- b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to

conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

21. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I

know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

22. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited

to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

### **Conclusion**

23. Based on the information set forth in this affidavit, I submit there is probable cause to believe that 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography) have been violated, and that evidence, instrumentalities, and/or contraband of this offense, more fully described in Attachment B, are located at the sites described in Attachment A1, A2, and/or A3. I respectfully request that this Court issue search warrants for the locations described in Attachments A1, A2, and A3, authorizing the search and seizure of the items described in Attachment B.

24. I am aware the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab; digital evidence will also undergo a similar process. For this reason, the “return” inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'B S Dean', written over a horizontal line.

Brian S. Dean  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to by phone on February 1, 2024.

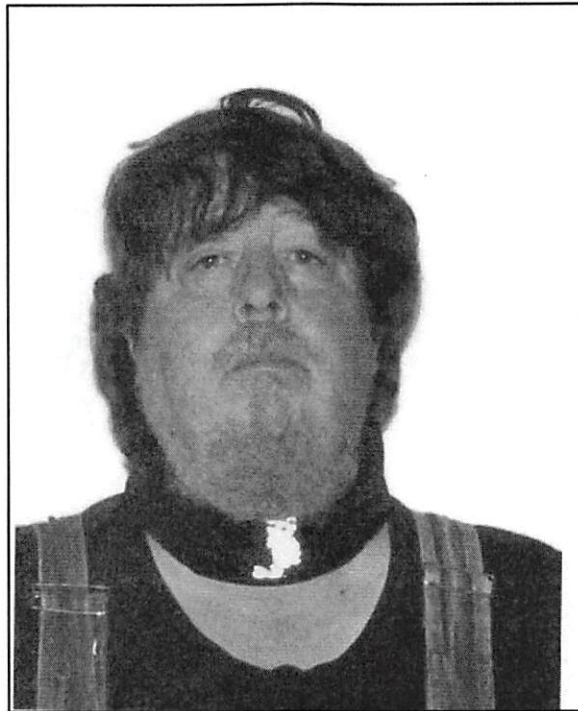
A handwritten signature in black ink, appearing to read 'Susan E. Huntsman', written over a horizontal line.

SUSAN E. HUNTSMAN  
UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A1**

**Person to be Searched**

The individual to be searched is **Bobby Neal Temple Jr.**, DOB: 09/04/1961, SSN: XXX-XX-5616. **TEMPLE** is reported to be approximately 6'2" tall and have brown hair and green eyes. **TEMPLE**'s driver's license photograph is displayed below.



**ATTACHMENT A2**

**Property to be Searched**

The property to be searched is a **black Chevrolet Silverado truck, Trail Boss edition, VIN: 1GCPYCEF1MZ308995 with a paper tag**, owned and operated by Bobby Neal Temple Jr. The photograph below was captured by law enforcement on 22 January 2024:



**ATTACHMENT A3**

**Property to be Searched**

The property to be searched is a residence located at **402 S. 14<sup>th</sup> St., Collinsville, OK 74021**, Northern District of Oklahoma, including outbuildings and vehicles on the curtilage premises. The main structure is located on the corner lot of E. 119<sup>th</sup> St. and S. 14<sup>th</sup> St., and is tan in color with reddish-brown trim and shingles. The photograph below was captured by law enforcement on 22 January 2024:



**ATTACHMENT B**

**Particular Things to be Seized**

All items that constitute evidence, instrumentalities, and/or contraband, of violations of Title 18, United States Code, Sections 2252(a)(4)(B) and (b)(2) (Possession of and Access with Intent to View Child Pornography), as it pertains to **Bobby Neal TEMPLE Jr.**, including:

- A. Images/videos/gifs of child pornography or child erotica; files containing images/videos/gifs; and data of any type relating to the sexual exploitation of minors or a sexual interest in children, material related to the possession thereof, and data of any type related to any person employing, using, persuading, inducing, enticing, or coercing any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting such visual depiction of such conduct, in any form wherever it may be stored or found including, but not limited to:
- i. Any cellular telephone, smartphone, tablet, personal digital assistant, computer, computer system and related peripherals; computer hardware; computer software; tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners,

monitors, printers, external storage devices, routers, modems, computer photographs, Graphic Interchange formats and/or photographs, undeveloped photographic film, slides, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to hardware, software, diskettes, backup tapes, CD-ROMS, DVD, Flash memory devices, and other storage mediums; any input/output peripheral devices, including but not limited to computer passwords and data security devices and computer-related documentation, and any hardware/software manuals related to or used to: visually depict child pornography; contain information pertaining to the interest in child pornography; and/or distribute, receive, or possess child pornography, or information pertaining to an interest in child pornography, or information pertaining to an interest in child pornography;

ii. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

iii. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children; and

iv. Stories, text-based files, motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit

conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;

B. Information, correspondence, records, documents or other materials pertaining to the possession, receipt or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256, or pertaining to the sexual exploitation of minors or a sexual interest in children, that were transmitted or received using computer, cellular device, personal digital assistant, or some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail including, but not limited to:

- i. Envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256 or relating to the sexual exploitation of minors or a sexual interest in children;
- ii. Books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256

or relating to the sexual exploitation of minors or a sexual interest in children;

- iii. Any and all records, documents, or materials, including any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States mail or by computer, any visual depiction of a minor engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256 or relating to the sexual exploitation of minors or a sexual interest in children;
- iv. Any and all records, documents, or materials, including any and all address books, names, and lists of names and addresses of minors visually depicted while engaging in sexually explicit conduct, defined in Title 18, United States Code, Section 2256; or relating to the sexual exploitation of minors or a sexual interest in children;
- v. Any and all records of Internet usage including user names and e-mail addresses and identities assumed for the purposes of communication on the Internet. These records may include billing and subscriber records, chat room logs, e-mail messages, and include electronic files in a computer and on other data storage mediums, including CDs or DVDs;

- vi. Any physical keys, encryption devices, dongles and similar physical items necessary to access computer equipment, storage devices or data;
  - vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data; and
  - viii. Files, records, programs, logs, electronic communications, scanning programs, financial records, hacking software, or router configuration software;
  - ix. Routers, modems, and network equipment used to connect computers to the Internet.
- C. Credit card information including, but not limited to, bills and payment records, and including, but not limited to, records of internet access;
- D. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence;
- E. Records or other items which evidence ownership or use of computer equipment or any of the devices described in this attachment that are found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes;
- F. Any and all adapters, chargers or other hardware items necessary to charge the battery, or to maintain the functioning of, any of the equipment described above; and

G. Any data or materials establishing ownership, use or control of any computer equipment seized from **402 S. 14<sup>th</sup> St., Collinsville, OK 74021**.

H. Any and all information, correspondence (including emails and text messages), records, documents and/or other materials related to contacts, in whatever form, with minors involving the production, possession and/or distribution of child pornography and the attempt or act of educating, enticing, coercing, or persuading a minor to engage in sexual acts.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term “computer” includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, instrumentalities, and/or contraband described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.